Semigroup Forum
DOI 10.1007/s00233-016-9783-z

RESEARCH ARTICLE

Ranks of finite semigroups of one-dimensional cellular automata

Alonso Castillo-Ramirez[1] · **Maximilien Gadouleau**[1]

Received: 5 October 2015 / Accepted: 22 February 2016

Abstract Since first introduced by John von Neumann, the notion of cellular automaton has grown into a key concept in computer science, physics and theoretical biology. In its classical setting, a cellular automaton is a transformation of the set of all configurations of a regular grid such that the image of any particular cell of the grid is determined by a fixed local function that only depends on a fixed finite neighbourhood. In recent years, with the introduction of a generalised definition in terms of transformations of the form $\tau : A^G \to A^G$ (where G is any group and A is any set), the theory of cellular automata has been greatly enriched by its connections with group theory and topology. In this paper, we begin the finite semigroup theoretic study of cellular automata by investigating the rank (i.e. the cardinality of a smallest generating set) of the semigroup $\mathrm{CA}(\mathbb{Z}_n; A)$ consisting of all cellular automata over the cyclic group $\mathbb{Z}_n$ and a finite set A. In particular, we determine this rank when n is equal to p, 2^k or $2^k p$, for any odd prime p and $k \geq 1$, and we give upper and lower bounds for the general case.

Keywords Cellular automata · Finite semigroups · Smallest generating sets

Communicated by Markus Lohrey.

✉ Alonso Castillo-Ramirez
alonso.castillo-ramirez@durham.ac.uk

Maximilien Gadouleau
m.r.gadouleau@durham.ac.uk

[1] School of Engineering and Computing Sciences, Durham University, South Road, Durham DH1 3LE, UK

Published online: 03 March 2016

1 Introduction

Cellular automata (CA) were introduced by John von Neumann as an attempt to design self-reproducing systems that were computationally universal (see [19]). Since then, the theory of CA has grown into an important area of computer science, physics, and theoretical biology (e.g. [4,12,20]). Among the most famous CA are Rule 110 and John Conway's Game of Life, both of which have been widely studied as discrete dynamical systems and are known to be capable of universal computation.

In recent years, many interesting results linking CA and group theory have appeared in the literature (e.g. see [3–5]). One of the goals of this paper is to embark in the new task of exploring CA from the point of view of finite semigroup theory.

We shall review the broad definition of CA that appears in [4, Sect. 1.4]. Let G be a group and A a set. Denote by A^G the set of functions of the form $x : G \to A$. For each $g \in G$, denote by $R_g : G \to G$ the right multiplication map, i.e. $(h)R_g := hg$ for any $h \in G$. We shall emphasise that in this paper we apply maps on the right, while in [4] maps are applied on the left.

Definition 1 Let G be a group and A a set. A *cellular automaton* over G and A is a map $\tau : A^G \to A^G$ satisfying the following property: there exists a finite subset $S \subseteq G$ and a *local map* $\mu : A^S \to A$ such that

$$(g)(x)\tau = ((R_g \circ x)|_S)\mu,$$

for all $x \in A^G$, $g \in G$, where $(R_g \circ x)|_S$ is the restriction to S of $(R_g \circ x) : G \to A$.

Let $\mathrm{CA}(G; A)$ be the set of all cellular automata over G and A; it is straightforward to show that, under composition of maps, $\mathrm{CA}(G; A)$ is a semigroup. Most of the literature on CA focus on the case when $G = \mathbb{Z}^d$, $d \geq 1$, and A is a finite set (see [12]). In this situation, an element $\tau \in \mathrm{CA}(\mathbb{Z}^d; A)$ is referred as a *d-dimensional* cellular automaton.

Although results on semigroups of CA have appeared in the literature before (see [10,18]), the semigroup structure of $\mathrm{CA}(G; A)$ remains basically unknown. In particular, the study of the finite semigroups $\mathrm{CA}(G; A)$, when G and A are finite, has been generally disregarded, perhaps because some of the classical questions are trivially answered (e.g. the Garden of Eden theorem becomes trivial). However, many new questions, typical of finite semigroup theory, arise in this setting.

One of the fundamental problems in the study of a finite semigroup M is the determination of the cardinality of a smallest generating subset of M; this is called the *rank* of M and denoted by $\mathrm{Rank}(M)$:

$$\mathrm{Rank}(M) := \min\{|H| : H \subseteq M \text{ and } \langle H \rangle = M\}.$$

It is well-known that, if X is any finite set, the rank of the full transformation semigroup $\mathrm{Tran}(X)$ (consisting of all functions $f : X \to X$) is 3, while the rank of the symmetric group $\mathrm{Sym}(X)$ is 2 (see [7, Ch. 3]). Ranks of various finite semigroups have been determined in the literature before (e.g. see [1,2,8,9,11]).

In order to hopefully bring more attention to the study of finite semigroups of CA, we shall propose the following problem.

Problem 1 For any finite group G and any finite set A, determine $\mathrm{Rank}(\mathrm{CA}(G; A))$.

A natural restriction of this problem, and perhaps a more feasible goal, is to determine the ranks of semigroups of CA over finite abelian groups.

In this paper we study the finite semigroups $\mathrm{CA}(\mathbb{Z}_n; A)$, where $\mathbb{Z}_n$ is the cyclic group of order $n \geq 2$ and A is a finite set with at least two elements. By analogy with the classical setting, we may say that the elements of $\mathrm{CA}(\mathbb{Z}_n; A)$ are one-dimensional cellular automata over $\mathbb{Z}_n$ and A.

In this paper we shall establish the following theorems.

Theorem 1 *Let $k \geq 1$ be an integer, p an odd prime, and A a finite set of size $q \geq 2$. Then:*

$$\mathrm{Rank}(\mathrm{CA}(\mathbb{Z}_p; A)) = 5;$$

$$\mathrm{Rank}(\mathrm{CA}(\mathbb{Z}_{2^k}; A)) = \begin{cases} \frac{1}{2}k(k+7), & \text{if} \quad q = 2; \\ \frac{1}{2}k(k+7)+2, & \text{if} \quad q \geq 3; \end{cases}$$

$$\mathrm{Rank}(\mathrm{CA}(\mathbb{Z}_{2^k p}; A)) = \begin{cases} \frac{1}{2}k(3k+17)+3, & \text{if} \quad q = 2; \\ \frac{1}{2}k(3k+17)+5, & \text{if} \quad q \geq 3. \end{cases}$$

Let $2\mathbb{Z}$ be the set of even integers. For any integer $n \geq 2$, let $[n] := \{1, 2, \ldots, n\}$. Denote by $\mathrm{d}(n)$ the number of divisors of n (including 1 and n itself) and by $\mathrm{d}_+(n)$ the number of even divisors of n. Let

$$E(n) := \left| \left\{ (s,t) \in [n]^2 : t \mid n, \ s \mid n, \ \text{and } t \mid s \right\} \right|$$

be the number of edges in the *divisibility digraph* of n (see Sect. 4).

Theorem 2 *Let $n \geq 2$ be an integer and A a finite set of size $q \geq 2$. Then:*

$$\mathrm{Rank}(\mathrm{CA}(\mathbb{Z}_n; A)) = \begin{cases} \mathrm{d}(n) + \mathrm{d}_+(n) + E(n) - 2 + \epsilon(n,2), & \text{if} \quad q = 2 \text{ and } n \in 2\mathbb{Z}; \\ \mathrm{d}(n) + \mathrm{d}_+(n) + E(n) + \epsilon(n,q), & \text{otherwise;} \end{cases}$$

where $0 \leq \epsilon(n,q) \leq \max\{0, \mathrm{d}(n) - \mathrm{d}_+(n) - 2\}$.

2 Preliminary results

For the rest of the paper, let $n \geq 2$ be an integer and A a finite set of size $q \geq 2$. We may assume that $A = \{0, 1, \ldots, q-1\}$. When G is a finite group, we may always assume that the finite subset $S \subseteq G$ of Definition 1 is equal to G, so any cellular automaton over G and A is completely determined by the local map $\mu : A^G \to A$. Therefore, if $|G| = n$, we have $|\mathrm{CA}(G; A)| = q^{q^n}$.

It is clear that $\mathrm{CA}(\mathbb{Z}_n; A)$ is contained in the semigroup of transformations $\mathrm{Tran}(A^n)$, where A^n is the n-th Cartesian power of A. For any $f \in \mathrm{Tran}(A^n)$ write $f = (f_1, \ldots, f_n)$, where $f_i : A^n \to A$ is the *i-th coordinate function of f*. For any semigroup M and $\sigma \in M$, define the *centraliser* of σ in M by

$$C_M(\sigma) := \{\tau \in M : \tau\sigma = \sigma\tau\}.$$

It turns out that $\mathrm{CA}(\mathbb{Z}_n; A)$ is equal to the centraliser of a certain transformation in $\mathrm{Tran}(A^n)$.

For any $f \in \mathrm{Tran}(A^n)$, define an equivalence relation $\sim$ on A^n as follows: for any $x, y \in A^n$, say that $x \sim y$ if and only if there exist $r, s \geq 1$ such that $(x)f^r = (y)f^s$. The equivalence classes induced by this relation are called the *orbits* of f.

Lemma 1 *Let $n \geq 2$ be an integer and A a finite set. Consider the map $\sigma : A^n \to A^n$ given by*

$$(x_1, \ldots, x_n)\sigma = (x_n, x_1, \ldots, x_{n-1}).$$

Then:

(i) $\mathrm{CA}(\mathbb{Z}_n; A) = C_{\mathrm{Tran}(A^n)}(\sigma) := \{\tau \in \mathrm{Tran}(A^n) : \tau\sigma = \sigma\tau\}$.
(ii) Let $\mathcal{O}$ be the set of orbits of $\sigma : A^n \to A^n$. For every $P \in \mathcal{O}$, $|P|$ divides n.
(iii) Every $\tau \in \mathrm{CA}(\mathbb{Z}_n; A)$ satisfies the following property: for every $P \in \mathcal{O}$ there exists $Q \in \mathcal{O}$, with $|Q|$ dividing $|P|$, such that $(P)\tau = Q$.

Proof We shall prove each part.

(i) By Definition 1, a map $\tau : A^n \to A^n$ is a cellular automaton over $G = \mathbb{Z}_n$ and A if and only if there exists a map $\mu : A^n \to A$ such that

$$(x_1, x_2, \ldots, x_n)\tau_i = (x_{1+i}, x_{2+i}, \ldots, x_{n+i})\mu$$

for any $1 \leq i \leq n$, where the sum in the subindex of x_{j+i} is done modulo n. Hence,

$$\begin{aligned}(x_1, x_2, \ldots, x_n)\sigma\tau &= (x_n, x_1, \ldots, x_{n-1})\tau \\ &= ((x_1, x_2, \ldots, x_n)\mu, (x_2, x_3, \ldots, x_1)\mu, \ldots, (x_n, x_1, \ldots, x_{n-1})\mu) \\ &= ((x_2, x_3, \ldots, x_1)\mu, (x_3, x_4, \ldots, x_2)\mu, \ldots, (x_1, x_2, \ldots, x_n)\mu)\sigma \\ &= (x_1, x_2, \ldots, x_n)\tau\sigma.\end{aligned}$$

This shows that $\mathrm{CA}(\mathbb{Z}_n; A) \leq \{\tau \in \mathrm{Tran}(A^n) : \tau\sigma = \sigma\tau\}$. Let $f \in \mathrm{Tran}(A^n)$ be such that $f\sigma = \sigma f$. This implies that $f\sigma^k = \sigma^k f$ for any $k \in \mathbb{Z}$, so

$$(x_1, x_2, \ldots, x_n)f_{n-k} = (x_{1-k}, x_{2-k}, \ldots, x_{n-k})f_n.$$

Therefore, f is a cellular automaton over $\mathbb{Z}_n$ and A with $\mu = f_n$.

(ii) This follows directly by the Orbit-Stabiliser Theorem ([6, Theorem 1.4A]).

(iii) Fix $\tau \in \mathrm{CA}(\mathbb{Z}_n; A)$, $P \in \mathcal{O}$ and $x \in P$. By definition of orbit, and since σ is a permutation, for every $y \in P$ there is $i \in \mathbb{Z}$ such that $(x)\sigma^i = y$. By part (i), $(x)\tau\sigma^i = (x)\sigma^i\tau = (y)\tau$, so $(P)\tau \subseteq Q$ for some $Q \in \mathcal{O}$. Furthermore, for every $z \in Q$ there is $j \in \mathbb{Z}$ such that $(z)\sigma^j = (x)\tau$, so $z = (x)\sigma^{-j}\tau \in (P)\tau$. This shows that $(P)\tau = Q$. Finally, we show that $|Q|$ divides $|P|$. Fix $z \in Q$. For any $w \in Q$ there is $k \in \mathbb{Z}$ such that $z = (w)\sigma^k$. Then σ^k is a bijection between the preimage sets $(z)\tau^{-1}$ and $(w)\tau^{-1}$. This means that $\left|(z)\tau^{-1}\right| = \left|(w)\tau^{-1}\right|$ for every $w \in Q = (P)\tau$. Therefore,

$$|P| = \sum_{w \in Q} \left|(w)\tau^{-1}\right| = \left|(z)\tau^{-1}\right| \cdot |Q| .$$

Lemma 1 (i) is in fact a particular case of a more general result.

Lemma 2 *Let G be a finite group and A a finite set. For each $g \in G$, let $\sigma_g \in \mathrm{Tran}(A^G)$ be the transformation defined by $(h)(x)\sigma_g := (hg^{-1})x$, for any $h \in G$, $x \in A^G$. Then,*

$$\mathrm{CA}(G; A) = \{\tau : A^G \to A^G : \tau\sigma_g = \sigma_g\tau,\ \forall g \in G\}.$$

Proof The result follows by Curtis-Hedlund Theorem (see [4, Theorem 1.8.1]).

Let $\mathrm{ICA}(G; A)$ be the set of invertible cellular automata:

$$\mathrm{ICA}(G; A) := \{\tau \in \mathrm{CA}(G; A) : \exists \phi \in \mathrm{CA}(G; A) \text{ such that } \tau\phi = \phi\tau = \mathrm{id}\}.$$

It may be shown that $\mathrm{ICA}(G; A) = \mathrm{CA}(G; A) \cap \mathrm{Sym}(A^G)$ whenever A is finite (see [4, Theorem 1.10.2]).

We shall use the cyclic notation to denote the permutations in $\mathrm{Tran}(A^n)$. If $D \subseteq A^n$ and $a \in A^n$, we define the transformation $(D \to a) \in \mathrm{Tran}(A^n)$ by

$$(x)(D \to a) := \begin{cases} a & \text{if } x \in D \\ x & \text{otherwise} . \end{cases}$$

When $D = \{b\}$ is a singleton, we write $(b \to a)$ instead of $(\{b\} \to a)$.

In the following examples, we identify the elements of A^n with their lexicographical order: $(a_1, a_2, \ldots, a_n) \sim \sum_{i=1}^{n} a_i q^{i-1}$.

Example 1 A generating set for $\mathrm{CA}(\mathbb{Z}_2; \{0, 1\})$ is

$$\{(1, 2),\ (\{1, 2\} \to 0),\ (0, 3),\ (3 \to 0)\},$$

where $0 := (0, 0)$, $1 := (1, 0)$, $2 := (0, 1)$ and $3 := (1, 1)$. Direct calculations in GAP show that indeed $\mathrm{Rank}(\mathrm{CA}(\mathbb{Z}_2; \{0, 1\})) = 4$.

Example 2 A generating set for CA $(\mathbb{Z}_3; \{0, 1\})$ is

$$\{(1,2,4)\,(0,7)\,,\ (1,6)\,(2,5)\,(3,4)\,,\ (1 \to 6)(2 \to 5)(4 \to 3),\ (\{1,2,4\} \to 0), (7 \to 0)\}.$$

Direct calculations in GAP show that indeed $\mathrm{Rank}(\mathrm{CA}(\mathbb{Z}_3; \{0, 1\})) = 5$.

If U is a subset of a finite semigroup M, the *relative rank* of U in M, denoted by $\mathrm{Rank}(M : U)$, is the minimum cardinality of a subset $V \subseteq M$ such that $\langle U, V \rangle = M$. The proof of the main results of this paper are based in the following observation.

Lemma 3 *Let G be a finite group and A a finite set. Then,*

$$\mathrm{Rank}(\mathrm{CA}(G; A)) = \mathrm{Rank}(\mathrm{CA}(G; A) : \mathrm{ICA}(G; A)) + \mathrm{Rank}(\mathrm{ICA}(G; A)).$$

Proof As $\mathrm{ICA}(G; A)$ is the group of units of $\mathrm{CA}(G; A)$, this follows by [1, Lemma 3.1]. □

In Sect. 3 we study the rank of $\mathrm{ICA}(\mathbb{Z}_n; A)$, while in Sect. 4 we study the relative rank of $\mathrm{ICA}(\mathbb{Z}_n; A)$ in $\mathrm{CA}(\mathbb{Z}_n; A)$.

3 The rank of ICA$(\mathbb{Z}_n; A)$

Let $\sigma : A^n \to A^n$ be as defined in Lemma 1. For any $d \geq 1$ dividing n, the number of orbits of σ of size d is given by the Moreau's necklace-counting function

$$\alpha(d, q) = \frac{1}{d} \sum_{b|d} \mu\left(\frac{d}{b}\right) q^b,$$

where μ is the classic Möbius function (see [14]). In particular, if $d = p^k$, where p is a prime number and $k \geq 1$, then

$$\alpha(p^k, q) = \frac{q^{p^k} - q^{p^{k-1}}}{p^k}. \tag{1}$$

Remark 1 Observe that $\alpha(d, q) = 1$ if and only if $(d, q) = (2, 2)$. Hence, the case when n is even and $q = 2$ is degenerate and shall be analysed separately in the rest of the paper.

We say that d is a non-trivial divisor of n if $d \mid n$ and $d \neq 1$ (note that, in our definition, $d = n$ is a non-trivial divisor of n). For any integer $\alpha \geq 1$, let Sym_α and Alt_α be the symmetric and alternating groups on $[\alpha] = \{1, \ldots, \alpha\}$, respectively.

A wreath product of the form $\mathbb{Z}_d \wr \mathrm{Sym}_\alpha := \{(v; \phi) : v \in (\mathbb{Z}_d)^\alpha, \phi \in \mathrm{Sym}_\alpha\}$ is called a *generalized symmetric group* (see [17]). We shall use the additive notation for the elements of $(\mathbb{Z}_d)^\alpha$, so the product in $\mathbb{Z}_d \wr \mathrm{Sym}_\alpha$ is

$$(v; \phi) \cdot (w; \psi) = (v + w^\phi; \phi\psi),$$

where $v, w \in (\mathbb{Z}_d)^\alpha$, $\phi, \psi \in \mathrm{Sym}_\alpha$, and ϕ acts on w by permuting the coordinates. We shall identify the elements $(v; \mathrm{id}) \in \mathbb{Z}_d \wr \mathrm{Sym}_\alpha$ with $v \in (\mathbb{Z}_d)^\alpha$.

The following result is a refinement of [18, Theorem 9].

Lemma 4 *Let $n \geq 2$ be an integer and A a finite set of size $q \geq 2$. Let $d_1, d_2, \ldots, d_\ell$ be the non-trivial divisors of n. Then*

$$\mathrm{ICA}(\mathbb{Z}_n; A) \cong (\mathbb{Z}_{d_1} \wr \mathrm{Sym}_{\alpha(d_1,q)}) \times \cdots \times (\mathbb{Z}_{d_\ell} \wr \mathrm{Sym}_{\alpha(d_\ell,q)}) \times \mathrm{Sym}_q.$$

Proof Let $\mathcal{O}$ the set of orbits of $\sigma : A^n \to A^n$ as defined in Lemma 1. Part (ii) of that lemma shows that $\mathrm{CA}(\mathbb{Z}_n; A)$ is contained in the semigroup

$$\mathrm{Tran}(A^n, \mathcal{O}) := \{f \in \mathrm{Tran}(A^n) : \forall P \in \mathcal{O},\ \exists Q \in \mathcal{O} \text{ such that } (P)f \subseteq Q\}.$$

As $\mathcal{O}$ contains q singletons and $\alpha(d_i, q)$ orbits of size $d_i \geq 2$, we know by [2, Lemma 2.1] that the group of units of $\mathrm{Tran}(A^n, \mathcal{O})$ is

$$S(A^n, \mathcal{O}) \cong (\mathrm{Sym}_{d_1} \wr \mathrm{Sym}_{\alpha(d_1,q)}) \times \cdots \times (\mathrm{Sym}_{d_\ell} \wr \mathrm{Sym}_{\alpha(d_\ell,q)}) \times \mathrm{Sym}_q.$$

Clearly, $\mathrm{ICA}(\mathbb{Z}_n; A) \leq S(A^n, \mathcal{O})$. Let P be an orbit of size d_i. Since the restriction of σ to P, denoted by $\sigma|_P$, is a cycle of length d_i, and the centraliser of $\sigma|_P$ in Sym_{d_i} is $\langle \sigma|_P \rangle \cong \mathbb{Z}_{d_i}$, it follows that

$$\mathrm{ICA}(\mathbb{Z}_n; A) \leq (\mathbb{Z}_{d_1} \wr \mathrm{Sym}_{\alpha(d_1,q)}) \times \cdots \times (\mathbb{Z}_{d_\ell} \wr \mathrm{Sym}_{\alpha(d_\ell,q)}) \times \mathrm{Sym}_q.$$

Equality follows as any permutation stabilising the sets of orbits of size d_i commutes with σ. □

For $1 \leq i \leq \alpha$, denote by e^i the element of $(\mathbb{Z}_d)^\alpha$ with 1 at the i-th coordinate, and 0 elsewhere. Denote by e^0 the element of $(\mathbb{Z}_d)^\alpha$ with 0's everywhere. For any $\alpha \geq 2$, define permutations $z_\alpha \in \mathrm{Sym}_\alpha$ by

$$z_\alpha := \begin{cases} (1, 2, 3, \ldots, \alpha), & \text{if } \alpha \text{ is odd,} \\ (2, 3, \ldots, \alpha) & \text{if } \alpha \text{ is even.} \end{cases} \tag{2}$$

Note that the order of z_α, denoted by $o(z_\alpha)$, is always odd.

In the following Lemma we determine the rank of the generalized symmetric group.

Lemma 5 *Let $d, \alpha \geq 2$. Then,* $\mathrm{Rank}\left(\mathbb{Z}_d \wr \mathrm{Sym}_\alpha\right) = 2$.

Proof It is clear that $\mathbb{Z}_d \wr \mathrm{Sym}_\alpha$ is not a cyclic group, so $2 \leq \mathrm{Rank}\left(\mathbb{Z}_d \wr \mathrm{Sym}_\alpha\right)$.

Define z_α as in (2). We will show that $\mathbb{Z}_d \wr \mathrm{Sym}_\alpha$ is generated by

$$x := (e^1; z_\alpha) \text{ and } y := (e^1; (1, 2)).$$

Let $M := \langle x, y \rangle \leq \mathbb{Z}_d \wr \mathrm{Sym}_\alpha$. Let $\rho : \mathbb{Z}_d \wr \mathrm{Sym}_\alpha \to \mathrm{Sym}_\alpha$ be the natural projection, and note that this is a group homomorphism. Clearly, $(M)\rho = \mathrm{Sym}_\alpha$ and

$\ker(\rho) = (\mathbb{Z}_d)^\alpha$, so, in order to prove that $M = \mathbb{Z}_d \wr \mathrm{Sym}_\alpha$, it suffices to show that $(\mathbb{Z}_d)^\alpha \leq M$.

Since $(M)\rho = \mathrm{Sym}_\alpha$, the intersection $(\mathbb{Z}_d)^\alpha \cap M$ is a Sym_α-invariant submodule of $(\mathbb{Z}_d)^\alpha$. If $\alpha = 2$, then $x = e^1$ generates $(\mathbb{Z}_d)^\alpha$ as Sym_α-module, so $(\mathbb{Z}_d^\alpha) \cap M = (\mathbb{Z}_d^\alpha)$. Henceforth, assume $\alpha \geq 3$. Observe that

$$y^2 = e^1 + e^2 = (1, 1, 0 \ldots, 0) \in (\mathbb{Z}_d)^\alpha \cap M.$$

Now, by Sym_α-invariance

$$\begin{aligned} &y^2 + \sum_{i=1}^{d-1} \left(y^2\right)^{(1,2,3)} + \left(y^2\right)^{(1,3,2)} \\ &\quad = (1, 1, 0, \ldots, 0) + (0, d-1, d-1, 0, \ldots, 0) + (1, 0, 1, 0, \ldots, 0) \\ &\quad = (2, 0, \ldots, 0) =: 2e^1 \in (\mathbb{Z}_d)^\alpha \cap M \end{aligned}$$

If d is odd, then $2e^1$ generates $(\mathbb{Z}_d)^\alpha$ as Sym_α-module, so $(\mathbb{Z}_d)^\alpha \cap M = (\mathbb{Z}_d)^\alpha$.

Suppose that d is even and α is odd. Then,

$$x^\alpha = (1, 1, \ldots, 1) \in (\mathbb{Z}_d)^\alpha \cap M.$$

Since Sym_α is 2-transitive on the basis of $(\mathbb{Z}_d)^\alpha$ and $y^2 = (1, 1, 0 \ldots, 0) \in (\mathbb{Z}_d)^\alpha \cap M$, we obtain that $(1, \ldots, 1, 0) \in (\mathbb{Z}_d)^\alpha \cap M$. Therefore,

$$(1, 1, \ldots, 1) - (1, \ldots, 1, 0) = (0, \ldots, 0, 1) \in (\mathbb{Z}_d)^\alpha \cap M,$$

and $(\mathbb{Z}_d)^\alpha \cap M = (\mathbb{Z}_d)^\alpha$.

Finally, suppose that d and α are both even. Then,

$$x^{\alpha-1} = (\alpha - 1, 0, \ldots, 0) \in (\mathbb{Z}_d)^\alpha \cap M.$$

Write $\alpha - 1 = 2k + 1$, for some $k \in \mathbb{N}$. Then

$$x^{\alpha-1} - \sum_{i=1}^{k} 2e^1 = (1, 0, \ldots, 0) \in (\mathbb{Z}_d)^\alpha \cap M.$$

Therefore, $(\mathbb{Z}_d)^\alpha \cap M = (\mathbb{Z}_d)^\alpha$. □

We need the following results in order to establish $\mathrm{Rank}(\mathrm{ICA}(\mathbb{Z}_p, A))$ when p is a prime number.

Lemma 6 (Lemma 5.3.4 in [13]) *Let $\alpha \geq 2$. The permutation module for Sym_α over a field $\mathbb{F}$ of characteristic p has precisely two proper nonzero submodules:*

$$U_1 := \{(a, a, \ldots, a) : a \in \mathbb{F}\} \text{ and } U_2 := \left\{(a_1, a_2, \ldots, a_\alpha) \in \mathbb{F}^\alpha : \sum_{i=1}^{\alpha} a_i = 0\right\}.$$

Theorem 3 ([15,16]) *Let $q \geq 3$ be an integer.*

(i) Except for $q \in \{5, 6, 8\}$, Sym_q is generated by an element of order 2 and an element of order 3.
(ii) If $p' > 3$ is a prime number dividing $q!$ and $q \neq 2p' - 1$, then Sym_q is generated by an element of order 2 and an element of order p'.

Lemma 7 *Let p be a prime number and A a finite set of size $q \geq 2$. Then:*

(i) If $q \geq 3$ and $p = 2$, then $\mathrm{Rank}(\mathrm{ICA}(\mathbb{Z}_2; A)) = 3$.
(ii) If $q \geq 2$ and $p \geq 3$, or $q = p = 2$, then $\mathrm{Rank}(\mathrm{ICA}(\mathbb{Z}_p; A)) = 2$.

Proof If $q = p = 2$, the result follows by Example 1. Assume $(p, q) \neq (2, 2)$. By Lemma 4,

$$\mathrm{ICA}(\mathbb{Z}_p; A) \cong W := (\mathbb{Z}_p \wr \mathrm{Sym}_\alpha) \times \mathrm{Sym}_q,$$

where $\alpha := \alpha(p, q) \geq 2$ is the Moreau's necklace-counting function. We use the basic fact that $\mathrm{Rank}(G/N) \leq \mathrm{Rank}(G)$, for any group G and any normal subgroup N of G. Let U_2 be the Sym_α-invariant submodule of $(\mathbb{Z}_p)^\alpha$ defined in Lemma 6. Then U_2 is a normal subgroup of $\mathbb{Z}_p \wr \mathrm{Sym}_\alpha$ such that $(\mathbb{Z}_p \wr \mathrm{Sym}_\alpha)/U_2 \cong \mathbb{Z}_p \times \mathrm{Sym}_\alpha$. Now, Alt_α is a normal subgroup of $\mathbb{Z}_p \times \mathrm{Sym}_\alpha$ with quotient $\mathbb{Z}_p \times \mathbb{Z}_2$. This implies that there is a normal subgroup N of $\mathbb{Z}_p \wr \mathrm{Sym}_\alpha$ with quotient isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_2$. Therefore, $N \times \mathrm{Alt}_q$ is a normal subgroup of W with quotient group isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Hence,

$$\mathrm{Rank}(\mathbb{Z}_p \times \mathbb{Z}_2 \times \mathbb{Z}_2) \leq \mathrm{Rank}(W). \tag{3}$$

Define z_α and z_q as in (2). We shall prove the two cases (i) and (ii).

(i) Suppose that $q \geq 3$ and $p = 2$, so $3 \leq \mathrm{Rank}(W)$ by (3). We shall show that $W = \langle v_1, v_2, v_3 \rangle$ where

$$\begin{aligned} v_1 &:= ((e^1; z_\alpha), \mathrm{id}), \\ v_2 &:= ((e^1; (1, 2)), z_q), \\ v_3 &:= ((e^0; \mathrm{id}), (1, 2)). \end{aligned}$$

The projections of v_1, v_2 and v_3 to Sym_q generate Sym_q, so it is enough to prove that v_1 and

$$(v_2)^{o(z_q)} = \begin{cases} ((e^1; (1, 2)), \mathrm{id}), & \text{if } o(z_q) = 1 \mod (4) \\ ((e^2; (1, 2)), \mathrm{id}), & \text{if } o(z_q) = 3 \mod (4) \end{cases}$$

generate $\mathbb{Z}_2 \wr \mathrm{Sym}_\alpha$. Let $M := \langle v_1, (v_2)^{o(z_q)} \rangle$. We follow a similar strategy as in the proof of Lemma 5. Note that the projections of v_1 and $(v_2)^{o(z_q)}$ to Sym_α generate Sym_α. Now, $(\mathbb{Z}_2)^\alpha \cap M$ is an Sym_α-invariant submodule of $(\mathbb{Z}_2)^\alpha$.
If α is even, then

$$(v_1)^{o(z_\alpha)} = (1, 0, \ldots, 0) = e^1 \in (\mathbb{Z}_2)^\alpha \cap M,$$

and so $(\mathbb{Z}_2)^\alpha \cap M = (\mathbb{Z}_2)^\alpha$ in this case.
Suppose that α is odd. Then

$$(v_1)^{o(z_\alpha)} = (1, 1, \ldots 1) \in (\mathbb{Z}_2)^\alpha \cap M.$$

Observe that

$$(v_2)^{2o(z_q)} = (1, 1, 0, \ldots, 0) \in (\mathbb{Z}_2)^\alpha \cap M.$$

By the 2-transitivity of Sym_α we obtain that $(0, 1, \ldots, 1) \in (\mathbb{Z}_2)^\alpha \cap M$. Therefore,

$$e^1 = (1, 1, \ldots, 1) + (0, 1, \ldots, 1) \in (\mathbb{Z}_2)^\alpha \cap M,$$

and we conclude that $(\mathbb{Z}_2)^\alpha \cap M = (\mathbb{Z}_2)^\alpha$ in this case as well.

(ii) Suppose that $q \geq 2$ and $p \geq 3$. Then $2 \leq \mathrm{Rank}(W)$ by (3). Observe that (1) implies that $\alpha = \frac{q^p - q}{p}$ is always an even number. We shall find generators u_1 and u_2 of W of the form

$$u_1 := ((e^1; (2, 3, \ldots, \alpha)), g) \text{ and } u_2 := ((e^1; (1, 2)), h), \tag{4}$$

where $g, h \in \mathrm{Sym}_q$, g is an involution, and $\langle g, h \rangle = \mathrm{Sym}_q$. As the projections of u_1 and u_2 to Sym_q generate Sym_q, it is enough to show that $(u_1)^2$ and $(u_2)^{o(h)}$ generate $\mathbb{Z}_p \wr \mathrm{Sym}_\alpha$. Let $M := \langle (u_1)^2, (u_2)^{o(h)} \rangle$. The projections of $(u_1)^2$ and $(u_2)^{o(h)}$ to Sym_α generate Sym_α, so, as in the proof of Lemma 5, it is enough to show that $(\mathbb{Z}_p)^\alpha \leq M$. Observe that $(\mathbb{Z}_p)^\alpha \cap M$ is a Sym_α-invariant subspace of $(\mathbb{Z}_p)^\alpha$.
We shall show that $(\mathbb{Z}_p)^\alpha \cap M$ is a nonzero Sym_α-invariant subspace of $(\mathbb{Z}_p)^\alpha$ different from U_1 and U_2, as given by Lemma 6, so $(\mathbb{Z}_p)^\alpha \cap M = M$. Whenever $\alpha \geq 3$, it suffices to show that at least one of the following elements of $(\mathbb{Z}_p)^\alpha \cap M$ is nonzero:

$$w_1 := (u_1)^{2(\alpha-1)} = (2(\alpha - 1), 0, \ldots, 0),$$
$$w_2 := (u_2)^{2o(h)} = (o(h), o(h), 0, \ldots, 0).$$

Let $q = 2$, and take $g := (1, 2)$ and $h := (1)$. The only case when $\alpha = 2$ is when $p = 3$. Here, although $w_2 = (1, 1)$ is nonzero, it generates U_1; however, $w_1 = (2, 0) \notin U_1 \cup U_2$, as required. For $p \geq 4$, $w_2 = (1, 1, 0, \ldots, 0)$ is always nonzero, as required. Henceforth, suppose $q \geq 3$.

Assume first that $p > 3$. For $q \notin \{5, 6, 8\}$, take g and h as the generators of Sym_q of orders 2 and 3, respectively, stated in Theorem 3 (i). Hence, $w_2 = (3, 3, 0, \ldots, 0)$ is nonzero.
For $q \in \{5, 6, 8\}$, take $g := (1, 2)$ and $h := z_q$ (as defined in (2)). If $q = 5$, then w_2 is nonzero, except when $p = 5$. In this case, by Eq. (1),

$$\alpha - 1 = \frac{5^5 - 5}{5} - 1 = 623 \neq 0 \mod (5),$$

so w_1 is nonzero. If $q = 6$, then w_2 is nonzero, except when $p = 5$. In this case,

$$\alpha - 1 = \frac{6^5 - 6}{5} - 1 = 1553 \neq 0 \mod (5),$$

so w_1 is nonzero. If $q = 8$, then w_2 is nonzero, except when $p = 7$. In this case,

$$\alpha - 1 = \frac{8^7 - 8}{7} - 1 = 299591 \neq 0 \mod (7),$$

so w_1 is nonzero.
Assume now that $p = 3$. If $q \geq 5$, then $5 \mid q!$ and, for $q \neq 2 \cdot 5 - 1 = 9$, we may take g and h as the generators of Sym_q of orders 2 and 5, respectively, stated in Theorem 3 (ii). Hence, w_2 is nonzero. If $q = 3$, $q = 4$, or $q = 9$, then

$$\alpha - 1 = \frac{3^3 - 3}{3} - 1 = 7 \neq 0 \mod (3),$$
$$\alpha - 1 = \frac{4^3 - 4}{3} - 1 = 19 \neq 0 \mod (3), \text{ or}$$
$$\alpha - 1 = \frac{9^3 - 9}{3} - 1 = 239 \neq 0 \mod (3),$$

respectively. Therefore, w_1 is nonzero, which completes the proof.

□

Recall that for any integer $n \geq 2$, we denote by $\mathrm{d}(n)$ the number of divisors of n (including 1 and n itself) and by $\mathrm{d}_+(n)$ the number of even divisors of n (so $\mathrm{d}_+(n) = 0$ if and only if n is odd).

Theorem 4 *Let $n \geq 2$ be an integer and A a finite set of size $q \geq 2$.*

(i) If n is not a power of 2, then

$$\mathrm{Rank}(\mathrm{ICA}(\mathbb{Z}_n; A)) = \begin{cases} \mathrm{d}(n) + \mathrm{d}_+(n) - 1 + \epsilon(n, 2) & \text{if } q = 2 \text{ and } n \in 2\mathbb{Z}; \\ \mathrm{d}(n) + \mathrm{d}_+(n) + \epsilon(n, q), & \text{otherwise;} \end{cases}$$

where $0 \leq \epsilon(n, q) \leq \mathrm{d}(n) - \mathrm{d}_+(n) - 2$.

(ii) If $n = 2^k$, then

$$\mathrm{Rank}(\mathrm{ICA}(\mathbb{Z}_{2^k}; A)) = \begin{cases} 2\mathrm{d}(2^k) - 2 = 2k & \text{if} \quad q = 2; \\ 2\mathrm{d}(2^k) - 1 = 2k + 1 & \text{if} \quad q \geq 3. \end{cases}$$

Proof Let $d_1, d_2, \ldots, d_\ell$ be the non-trivial divisors of n, with $\ell = \mathrm{d}(n) - 1$, and let

$$\mathrm{ICA}(\mathbb{Z}_n; A) \cong W := (\mathbb{Z}_{d_1} \wr \mathrm{Sym}_{\alpha(d_1,q)}) \times \cdots \times (\mathbb{Z}_{d_\ell} \wr \mathrm{Sym}_{\alpha(d_\ell,q)}) \times \mathrm{Sym}_q.$$

Suppose first that $q \neq 2$ or n is odd. Then $\alpha(d_i, q) \geq 2$ for all i. As in the proof of Lemma 7, there is a normal subgroup $U \trianglelefteq \mathbb{Z}_{d_i} \wr \mathrm{Sym}_{\alpha(d_i,q)}$ with quotient group $\mathbb{Z}_{d_i} \times \mathrm{Sym}_{\alpha(d_i,q)}$, and $\mathrm{Alt}_{\alpha(d_i,q)}$ is a normal subgroup of $\mathbb{Z}_{d_i} \times \mathrm{Sym}_{\alpha(d_i,q)}$ with quotient group $\mathbb{Z}_{d_i} \times \mathbb{Z}_2$. Hence, there is a normal subgroup N_{d_i} of $\mathbb{Z}_{d_i} \wr \mathrm{Sym}_{\alpha(d_i,q)}$ with quotient isomorphic to $\mathbb{Z}_{d_i} \times \mathbb{Z}_2$. Therefore, $N_{d_1} \times \cdots \times N_{d_\ell}$ is a normal subgroup of W with quotient isomorphic to

$$Q := (\mathbb{Z}_{d_1} \times \mathbb{Z}_2) \times \cdots \times (\mathbb{Z}_{d_\ell} \times \mathbb{Z}_2) \times \mathbb{Z}_2.$$

If n is odd, then $\gcd(2, d_i) = 1$ for all i, so

$$Q \cong \mathbb{Z}_{2d_1} \times \cdots \times \mathbb{Z}_{2d_\ell} \times \mathbb{Z}_2,$$

and $\mathrm{Rank}(Q) = \ell + 1 = \mathrm{d}(n)$ in this case. If n is even, suppose that $d_1, \ldots, d_e$, with $e = \mathrm{d}_+(n)$, are all the even divisors of n. Hence,

$$Q \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_e} \times \mathbb{Z}_{2d_{e+1}} \times \cdots \times \mathbb{Z}_{2d_\ell} \times (\mathbb{Z}_2)^{e+1},$$

and $\mathrm{Rank}(Q) = \ell + e + 1 = \mathrm{d}(n) + \mathrm{d}_+(n)$. This gives the lower bound for the rank of W.

For the upper bound, we shall use the basic fact that $\mathrm{Rank}(G_1 \times G_2) \leq \mathrm{Rank}(G_1) + \mathrm{Rank}(G_2)$, for any pair of groups G_1 and G_2. Assume first that n is not a power of 2 and let d_ℓ be an odd prime. Hence, $\mathrm{Rank}\left((\mathbb{Z}_{d_\ell} \wr \mathrm{Sym}_{\alpha(d_\ell,q)}) \times \mathrm{Sym}_q\right) = 2$ by Lemma 7 (ii), and $\mathrm{Rank}(\mathbb{Z}_{d_i} \wr \mathrm{Sym}_{\alpha(d_i,q)}) = 2$ for all i by Lemma 5. Thus, $\mathrm{Rank}(W) \leq 2\ell = 2\mathrm{d}(n) - 2$. If n is a power of 2, then $\mathrm{Rank}\left((\mathbb{Z}_2 \wr \mathrm{Sym}_{\alpha(2,q)}) \times \mathrm{Sym}_q\right) = 3$ by Lemma 7 (i), so $\mathrm{Rank}(W) \leq 2\ell + 1 = 2\mathrm{d}(n) - 1$.

When $q = 2$ and n is even, we may assume that $d_\ell = 2$, so $\mathrm{ICA}(\mathbb{Z}_n; A) \cong (\mathbb{Z}_{d_1} \wr \mathrm{Sym}_{\alpha(d_1,2)}) \times \cdots \times (\mathbb{Z}_{d_{\ell-1}} \wr \mathrm{Sym}_{\alpha(d_{\ell-1},2)}) \times (\mathbb{Z}_2)^2$. The rest of the proof is similar to the previous paragraphs. □

Corollary 1 *Let p be an odd prime and $k \geq 1$ an integer. Let A be a finite set of size $q \geq 2$. Then:*

$$\mathrm{Rank}(\mathrm{ICA}(\mathbb{Z}_{2^k p}; A)) = \begin{cases} 4k + 1 & \text{if} \quad q = 2, \\ 4k + 2 & \text{if} \quad q \geq 3. \end{cases}$$

Proof This follows by Theorem 4 (i) because $\mathrm{d}(2^k p) - \mathrm{d}_+(2^k p) - 2 = 0$, so $\epsilon(2^k p, q) = 0$. □

4 The relative rank of ICA($\mathbb{Z}_n$; A) in CA($\mathbb{Z}_n$; A)

For any integer $n \geq 2$, define the *divisibility digraph of* n as the digraph with vertices $\mathcal{V} := \{s \in [n] : s \mid n\}$ and edges $\mathcal{E} := \{(s,t) \in \mathcal{V}^2 : t \mid s\}$. Denote $E(n) := |\mathcal{E}|$.

Lemma 8 *Let $n \geq 2$. If $n = p_1^{a_1} p_2^{a_2} \dots p_m^{a_m}$, where p_i are distinct primes, then*

$$E(n) = \frac{1}{2^m} \prod_{i=1}^{m} (a_i + 1)(a_i + 2).$$

Proof Note that the outdegree of any $s = p_1^{b_1} p_2^{b_2} \dots p_m^{b_m} \mid n$ is

$$\mathrm{outdeg}(s) = (b_1 + 1)(b_2 + 1) \dots (b_m + 1).$$

Therefore,

$$\begin{aligned} E(n) &= \sum_{s|n} \mathrm{outdeg}(s) = \sum_{b_1=0}^{a_1} \cdots \sum_{b_m=0}^{a_m} (b_1 + 1)(b_2 + 1) \dots (b_m + 1) \\ &= \frac{1}{2^m} \prod_{i=1}^{m} (a_i + 1)(a_i + 2). \end{aligned}$$

□

In the proof of the following result we shall use the notion of *kernel* of a transformation $\tau : A^n \to A^n$ as the partition of A^n induced by the equivalence relation $\{(x, y) \in A^n \times A^n : (x)\tau = (y)\tau\}$.

Lemma 9 *Let $n \geq 2$ be an integer and A a finite set of size $q \geq 2$. Then:*

$$\mathrm{Rank}(\mathrm{CA}(\mathbb{Z}_n; A) : \mathrm{ICA}(\mathbb{Z}_n; A)) = \begin{cases} E(n) - 1 & \text{if } \ q = 2 \text{ and } n \in 2\mathbb{Z}; \\ E(n) & \text{otherwise.} \end{cases}$$

Proof Let $\mathcal{O}$ be the set of orbits of $\sigma : A^n \to A^n$, as defined in Lemma 1. Let $d_1, \dots, d_\ell$ be all the divisors of n ordered as follows

$$1 = d_1 < d_2 < \cdots < d_{\ell-1} < d_\ell = n.$$

For $1 \leq i \leq \ell$, let $\alpha_i := \alpha(d_i, q)$ and denote by $\mathcal{O}_i$ the subset of $\mathcal{O}$ of orbits of size d_i. Let

$$B_i := \bigcup_{P \in \mathcal{O}_i} P.$$

Suppose that $q \neq 2$ or n is odd, so $\alpha_i \geq 2$ for all i. For any pair of divisors d_j and d_i such that $d_j \mid d_i$, fix $\omega_j \in B_j$ and $\omega_i \in B_i$ in distinct orbits. Denote the orbits that contains ω_i by $[\omega_i]$. Define idempotents $\tau_{i,j} \in \mathrm{CA}(\mathbb{Z}_n; A)$ in the following way:

$$(x)\tau_{i,j} := \begin{cases} (\omega_j)\sigma^k & \text{if} \quad x = (\omega_i)\sigma^k \\ x & \text{if} \quad x \in A^n \setminus [\omega_i]. \end{cases}$$

Note that $\tau_{i,j}$ collapses $[\omega_i]$ to $[\omega_j]$ and fixes everything else.

We claim that

$$H := \left\langle \mathrm{ICA}(\mathbb{Z}_n; A), \tau_{i,j} : d_j \mid d_i \right\rangle = \mathrm{CA}(\mathbb{Z}_n; A).$$

Let $\xi \in \mathrm{CA}(\mathbb{Z}_n; A)$. For $1 \leq i \leq \ell$, and define

$$(x)\xi_i := \begin{cases} (x)\xi & \text{if} \quad x \in B_i \\ x & \text{otherwise.} \end{cases}$$

Clearly $\xi_i \in \mathrm{CA}(\mathbb{Z}_n; A)$. By Lemma 1, we have $(B_i)\xi \subseteq \bigcup_{j \leq i} B_i$, so

$$\xi = \xi_1 \xi_2 \dots \xi_\ell.$$

We shall prove that $\xi_i \in H$ for all $1 \leq i \leq \ell$. For each i, decompose $B_i = B_i' \cup B_i''$, where

$$B_i' = \bigcup \left\{ P \in \mathcal{O}_i : (P)\xi_i \subseteq B_j \text{ for some } j < i \right\},$$
$$B_i'' = \bigcup \left\{ P \in \mathcal{O}_i : (P)\xi_i \subseteq B_i \right\}.$$

If ξ_i' and ξ_i'' are the transformations that act as ξ_i on B_i' and B_i'', respectively, and fix everything else, then $\xi_i = \xi_i' \xi_i''$.

1. We show that $\xi_i' \in H$. For any orbit $P \subseteq B_i'$, the orbit $Q := (P)\xi_i'$ is contained in B_j for some $j < i$. By Lemma 4, there is $\phi \in \mathrm{Sym}_{\alpha_i} \times \mathrm{Sym}_{\alpha_j} \leq \mathrm{ICA}(\mathbb{Z}_n; A)$ such that ϕ_s acts as the double transposition $([\omega_i], P_s)([\omega_j], Q_s)$, and

$$(P)\xi_i' = (P)\phi^{-1}\tau_{i,j}\phi.$$

   As ξ_i' may be decomposed as a product of transformations that only move one orbit in B_i', the above equality implies that $\xi_i' \in H$.
2. We show that $\xi_i'' \in H$. In this case, $\xi_i''|_{B_i} \in \mathrm{Tran}(B_i)$. In fact, as ξ_i'' preserves the partition of B_i into orbits, $\xi_i''|_{B_i} \in \langle \sigma|_{B_i} \rangle \wr \mathrm{Tran}_{\alpha_i}$. As $\alpha_i \geq 2$, the semigroup Tran_{α_i} is generated by $\mathrm{Sym}_{\alpha_i} \leq \mathrm{ICA}(\mathbb{Z}_n; A)$ together with the idempotent $\tau_{i,i}$. Hence, $\xi_i'' \in H$.

This establishes that the relative rank of $\mathrm{ICA}(\mathbb{Z}_n; A)$ in $\mathrm{CA}(\mathbb{Z}_n; A)$ is at most $E(n)$.

For the converse, suppose that

$$\langle \mathrm{ICA}(\mathbb{Z}_n; A), U\rangle = \mathrm{CA}(\mathbb{Z}_n; A),$$

where $|U| < E(n)$. Hence, we may assume that, for some $d_j \mid d_i$,

$$U \cap \langle \mathrm{ICA}(\mathbb{Z}_n; A), \tau_{i,j}\rangle = \emptyset. \tag{5}$$

By Lemma 1, there is no $\tau \in \mathrm{CA}(\mathbb{Z}_n; A)$ such that $(X)\tau \subseteq Y$ for $X \in \mathcal{O}_a$, $Y \in \mathcal{O}_b$ with $d_b \nmid d_a$. This, together with (5), implies that U has no element with kernel of the form

$$\big\{\{x, y\}, \{z\} : x \in P, y \in Q, z \in A^n \setminus (P \cup Q)\big\}$$

for any $P \in \mathcal{O}_i$, $Q \in \mathcal{O}_j$. Thus, there is no element in $\langle \mathrm{ICA}(\mathbb{Z}_n; A), U\rangle$ with kernel of such form, which is a contradiction (because $\tau_{i,j} \in \mathrm{CA}(\mathbb{Z}_n; A)$ has indeed this kernel).

The case when $q = 2$ and n is even follows similarly, except that now, as there is a unique orbit of size 2 in $\mathcal{O}$, there is no idempotent $\tau_{2,2}$. □

Finally, Theorems 1 and 2 follow by Theorem 4 and Lemmas 3, 7, 8 and 9.

Acknowledgments This work was supported by the EPSRC grant EP/K033956/1. We thank the helpful and insightful comments of the referee of this paper.

References

1. Araújo, J., Schneider, C.: The rank of the endomorphism monoid of a uniform partition. Semigroup Forum **78**, 498–510 (2009)
2. Araújo, J., Bentz, W., Mitchell, J.D., Schneider, C.: The rank of the semigroup of transformations stabilising a partition of a finite set. Math. Proc. Camb. Philos. Soc. **159**(02), 339–353 (2015)
3. Bartholdi, L.: Gardens of eden and amenability on cellular automata. J. Eur. Math. Soc. **12**, 241–248 (2010)
4. Ceccherini-Silberstein, T., Coornaert, M.: Cellular Automata and Groups. Springer Monographs in Mathematics. Springer, Berlin (2010)
5. Ceccherini-Silberstein, T.G., Machì, A., Scarabotti, F.: Amenable groups and cellular automata. Ann. Inst. Fourier **49**, 673–685 (1999)
6. Dixon, J.D., Mortimer, B.: Permutation Groups. Graduate Texts in Mathematics, vol. 163. Springer, New York (1996)
7. Ganyushkin, O., Mazorchuk, V.: Classical Finite Transformation Semigroups: An Introduction. Springer, London (2009)
8. Gomes, G.M.S., Howie, J.M.: On the ranks of certain finite semigroups of transformations. Math. Proc. Camb. Phil. Soc. **101**, 395–403 (1987)
9. Gray, R.D.: The minimal number of generators of a finite semigroup. Semigroup Forum **89**, 135–154 (2014)

10. Hartman, Y.: Large semigroups of cellular automata. Ergod. Theory Dyn. Syst. **32**(6), 1991–2010 (2012)
11. Howie, J.M., McFadden, R.B.: Idempotent rank in finite full transformation semigroups. Proc. R. Soc. Edinb. **114A**, 161–167 (1990)
12. Kari, J.: Theory of cellular automata: a survey. Theoret. Comput. Sci. **334**, 3–33 (2005)
13. Kleidman, P., Liebeck, M.: The Subgroup Structure of the Finite Classical Groups. London Mathematical Society Lecture Note Series, vol. 129. Cambridge University Press, Cambridge, MA (1990)
14. Metropolis, N., Rota, G.: Witt vectors and the algebra of necklaces. Adv. Math. **50**, 95–125 (1983)
15. Miller, G.A.: On the groups generated by two operators. Bull. Am. Math. Soc. **7**(10), 424–426 (1901)
16. Miller, G.A.: Possible orders of two generators of the alternating and of the symmetric group. Trans. Am. Math. Soc. **30**, 24–32 (1928)
17. Osima, M.: On the representations of the generalized symmetric group. Math. J. Okayama Univ. **4**, 39–56 (1954)
18. Salo, V.: Groups and monoids of cellular automata. In: Cellular Automata and Discrete Complex Systems. Lecture Notes in Computer Science, vol. 9099, pp. 17–45 (2015)
19. von Neumann, J.: Theory of self-reproducing automata. In: Burks, A.W. (ed.). University of Illinois Press, Champign, IL (1966)
20. Wolfram, S.: Computation theory of cellular automata. Commun. Math. Phys. **96**, 15–57 (1984)